

Hur skyddar Sharebook dina uppgifter

Ny Dataskyddsförordning GDPR

Den 25 maj 2018 träder EU:s nya dataskyddsförordning i kraft. Genom att EU samordnar och harmoniserar lagstiftningen avseende personuppgiftsskydd skall det bli enklare för enskilda individer inom EU att känna till vilka rättigheter man har. Samma lagstiftning gäller för personuppgiftsbehandling i alla länder som behandlar EU-medborgares personuppgifter.

Sharebook-systemet är anpassat för de nya reformerna för att uppfylla dataskydd och processer i enlighet med förordningens krav.

Vad gäller för dig som använder Sharebook?

Eftersom du och din organisation samlar in och behandlar uppgifter om (fysiska) personer är det ni som är personregisteransvariga. Sharebook är den tekniska plattformen som hjälper er att hantera uppgifterna i enlighet med ert syfte.

Därför är det er uppgift att berätta för era registrerade varför ni vill samla in personuppgifter och för vilket syfte.

Detta görs enklast genom att ni uppgör en registerbeskrivning (se www.tietosuoja.fi/sv) där ni meddelar t.ex. vem hos er som är ansvarig för insamlingen, samt varför och hur data insamlas och behandlas. En registerbeskrivning bör vara tillgänglig för de registrerade. Enklast är att ni publicerar denna på er hemsida, eller sänder beskrivningen till era registrerade.

T.ex. måste ni meddela ifall ni, av någon orsak, lämnar ut de insamlade personuppgifterna till någon annan part för marknadsföringsändamål eller något annat syfte. Ni skall även berätta hur länge ni sparar personuppgifterna och hur de registrerade kan ta del av och eventuellt korrigera sina uppgifter.

Ni ansvarar med andra ord för att:

1. Ni har rätt att samla in uppgiften och med vilken rätt (t.ex. för att kunna fakturera ett avtal)
2. Ni samlar in sådana uppgifter som behövs. Varken mer eller mindre.
3. NI har korrekta uppgifter om den registrerade och raderar personuppgifter som inte längre behövs.
4. Ni kan bevisa till den registrerade er rätt att inneha personuppgifter samt presentera vilka uppgifter om personen som ni har i registret.
5. Ni hanterar personuppgifterna säkert och skyddat från insyn.

Som personregisteransvariga är ni skyldiga att känna till den nya dataskyddsförordningen och dess innehåll. Eftersom förordningen gäller för alla EU-länder och -medborgare finns det en uppsjö med information på webben både på svenska, finska och engelska. Det lönar sig att hålla sig uppdaterad.

Beroende på vilken bransch ni verkar inom för att samla in personuppgifter finns det lite olika regler och rekommendationer. Vi rekommenderar er att kontakta er jurist eller branschorganisation för att få närmare vägledning för just er situation. Vissa organisationer måste utföra konsekvensbedömningar och tillsätta ett dataskyddsombud (DPO) om omfattningen av insamlingen är stor eller berör särskilda kategorier som kan anses vara känsliga (t.ex. hälso- och sjukvård).

Här finns en enkel Kom-ihåg-lista för att komma vidare



Vilka övriga program och tjänster använder ni?

Det är också viktigt för din organisation att dokumentera vilka typer av system, program och processer ni använder er av i insamlingen och behandlingen av personuppgifterna.

I de Allmänna villkoren för Sharebook kan du läsa om ansvarsfördelningen gällande hanteringen av personuppgifter då ni använder tjänsterna i Sharebook.

När ni använder andra leverantörer för behandling eller lagring av personuppgifter bör ni upprätta ett **registerbiträdesavtal** med dessa för att säkerställa att leverantören följer förordningen och era instruktioner.

Sharebook och säkerheten

Användarvänlighet, datasäkerhet och skydd av individers integritet är av största vikt för oss som arbetar med Sharebook. Inom företaget har vi en intern datasäkerhetspolicy och alla anställda är underställda sekretessbestämmelser samt skall följa företagets kvalitetspolicy och -reglemente.

För våra datamiljöer finns särskilda bestämmelser från vilka vi redogör nedan i korthet.

Fysisk miljö

Plattformen är installerad i två, geografiskt åtskilda serverhallar med fiberanslutning mellan hallarna och Gbps bandbredd mot Internet.

Strömförsörjningen är kompletterad med UPS samt dieselgenerator för att trygga tillgängligheten.

Samtliga servrar ingår i företagets underhållssystem med avseende på uppdaterings/uppgraderingsrutiner, säkerhetsgranskning, integritetsövervakning och övriga säkerhetsrutiner.

Normala uppdateringar sker löpande enligt schema och tack vare den redundanta lösningen kan dessa i de allra flesta installeras utan driftsavbrott.

Backuper/säkerhetskopior

Backuper av hela miljön tas dagligen och dessa lagras i de två separata serverhallarna på ett sådant sätt att hela miljön, jämte data, finns säkerhetskopierad på bägge platser.

Varje månad körs backuper enligt 3-2-1-strategin. D.v.s. att backuper tas i tre olika kopior varav 2 finns lokalt i serverhallarna och 1 kopia sparas på band som förvaras utanför de två serverhallarna.

Varje år sparas även kopior på backuper i ett bankfack, dessa lagras i 10 år.

Skalskydd

I skalskyddet ingår inbrotts-/brandlarm, övervakning av temperatur. Endast behörig personal har tillgång till hallarna och åtkomsten sker via lås försedda med kod/taggar.

Säkerhet och underhåll

Servermiljön är skyddad med redundanta brandväggar med IPS-skydd (Intrusion Prevention System) som identifierar attacker och intrångsförsök av olika slag. Miljön är även skyddad av lokala brandväggar på varje server.

Övervakning sker dygnet runt med avseende på tillgänglighet och för att identifiera potentiella säkerhetsproblem. Vidare sker en realtidsövervakning av servrarna som identifierar tecken på intrång eller otillbörlig användning av systemen.

De vitala loggar som utgör basen för en audit-trail sparas på en separat loggserver för att garantera att loggarna existerar i orörd form.

Vidare finns även ett system för att upprätthålla den säkerhetspolicy som vi internt arbetar med för att garantera högsta möjliga skydd på servernivå. Avvikelser från denna policy rapporteras till ansvariga personer per automatik. Vidare sker antivirus-/rootkit-scanningar dagligen på samtliga servrar.

Servrarna är konfigurerade med auditloggning och tillgången till servrarna, och därmed systemen, är begränsad till endast behörig personal.

Överföring av uppgifter till tredje part eller utanför EU

All hantering och lagring av persondata sker inom Finlands gränser. Sharebook överför aldrig uppgifter till tredje part eller nyttjar underleverantörer utan kundens uttryckliga vilja och samtycke. En sådan överföring kan t.ex. gälla utsändning av brev eller meddelanden som kunden initierat eller rapportering till myndigheter på kundens order.

Avtal om registerbiträde

Inom ramen för de Allmänna villkoren för Sharebook har vi beskrivit de ansvarsuppgifter som är fördelade på dig, som kund, och på oss – Sharebook. I villkoren framgår dina skyldigheter och vårt ansvar.

I samband med tecknande av avtal med Sharebook har parterna godkänt de Allmänna villkoren i vilket regleras registerbitrådets ansvar.